CYBERSCOUT®
Case Study

STATE MOVES TO PROTECT ELECTION INTEGRITY AND VOTER DATA

Industry Type: State Government
Business Size: Over 4 Million
Breach: No
Affected Individuals: None

2016 Presidential Election Illustrates Threat to State's Electoral Process

In the summer of 2016, when the Federal Bureau of Investigation warned state governments that hackers were attempting to access voter registration systems, one state's Election Board decided it was time to implement stricter information security systems and processes. The state wanted to avoid situations that happened in other areas: compromised voter rolls, voting infrastructures and breaches facilitated by third-party vendors.

The state hadn't suffered from a hacking incident, nor a loss of data. It's Election Board sought to show that the electoral process was as free, fair and secure as at any other time in history.

"We understood that it would be vital to hold each new technology or process to our high standards for data security. We were especially interested in CyberScout's ability to monitor the new technologies we planned to integrate into our infrastructure for unexpected issues." - Secretary of State

How CyberScout Helped

The state was especially concerned with accidentally introducing new security holes as it added new technologies and processes. So, it awarded CyberScout a single-source contract to:

- **Review all technologies** under consideration, design or implementation for configurations that didn't comply with the state's security practices.
- **Monitor changes to the state's network** for correct and comprehensive implementation, and signs of new vulnerabilities.
- **Provide technical advice** to a vendor-selection board.
- **Visit and assess each county's voting machines** to confirm their ability to protect voter data and the Election Board's network, and define security protocols for the consistent setup, management and takedown of the State's voting machines across all precincts.

Each new technology the state decides to incorporate into its election system introduces the possibility of new vulnerabilities. CyberScout managed and monitored implementation of new equipment and technologies to ensure that the state's plans for improving the integrity of their electoral process were fully executed.

CYBERSCOUT®
Case Study

Resolution

With the 2018 mid-term election looming on the horizon, the state's Election Board has a clear, actionable plan. CyberScout will stay engaged for as long as necessary to secure the state's voter rolls and electoral process. CyberScout will provide support services for the complete implementation of our recommendations, including penetration testing, vulnerability assessment, and advising on executing a results-based audit for elections with a firm grounding in actuarial best practices.

"Originally, we weren't expecting CyberScout to help us refine our auditing processes. But now we understand that that's one of their key competencies. We're glad for their insight, in addition to their help improving the security and privacy of our whole election process." - Secretary of State

State Moves to Protect Election Integrity and Voter Data

During the 2016 presidential election, one state's Election Board decided that it was time to implement stricter information security systems and processes in its election system. The state was especially concerned with introducing new security holes accidentally as it added new technologies and processes. So, it awarded CyberScout a single-source engagement to assist with reviewing new initiatives for security holes, provide technical advice to a vendor-selection board, and assess each county's voting machines to confirm their technology would protect voter data and the Election Board's network. With the 2018 mid-term election looming, CyberScout will stay engaged for as long as necessary to secure the state's voter rolls and electoral process.